УМНОЖИТЕЛИ ДЛЯ ПРОЦЕССОРОВ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ.

Ивашко А.В., Лунин Д.А.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Многие прикладные задачи, решение которых возможно только с помощью суперкомпьютеров, зачастую требуют работы с многоразрядными числами. В настоящее время позиционные методы вычисления над многоразрядными числами являются неэффективными. Также, ввиду непрерывного роста размерностей задач и требований, которые они предъявляют к точности решения, вытекает острая необходимость разработки новых методов для эффективного выполнения параллельных вычислений над многоразрядными числами.

Арифметика системы остаточных классов (СОК) нашла большое применение в многочисленных теоретико-числовых преобразованиях (ТЧП), которые широко используются для вычислений сверток/корреляций, криптографических алгоритмов и моделей отказоустойчивых цифровых систем. Для реализации арифметики СОК наиболее часто применяются специализированные цифровые сигнальные процессоры.

Арифметика по модулю 2^n+1 используется в некоторых приложениях, такие как, арифметика СОК, преобразование Ферма, для устранения ошибок округления при вычислении свёртки, и криптографических (символьных) алгоритмах. Для реализации этих приложений, было предложено несколько арифметических блоков по модулю 2^n+1.

Умножитель по модулю (2^n+1) играет важную роль в числовых преобразованиях Ферма и системах счисления в остатках; было выявлено, что представление чисел в коде «diminished-1» наиболее подходящее для представления элементов кольца. Существуют алгоритмы для умножения по модулю (2^n+1) использующие рекурсивные сумматоры по модулю (2^n+1), или регулярные бинарные интегрированные умножители с операцией приведения по модулю. Несмотря на то, что наиболее часто принимаются большое значение n, этот последний подход требует преобразования между кодом «diminished-1» и двоичным представлением.

Предлагается использовать параллельную модульную архитектуру умножителя по модулю (2^n+1) основанную на дереве Уоллеса, которая не требуют никакого преобразования. Используя дерево Уоллеса, можно значительно улучшить скорость умножителя. Эта архитектура демонстрирует повышенную модульность структуры и преимущества связанные с СБИС реализацией. Критическая задержка и аппаратные требования этого умножителя хорошо корреспондируются с бинарным умножителем.